Congressman Christopher Smith Statement for Hearing on "The Internet in China: A Tool for Freedom or Suppression?"

February 15, 2006

Good morning and welcome to this hearing on the Internet in China. We are here to examine a problem that is deeply troubling to me, and I believe, to the American people: that American technology and know-how is substantially enabling repressive regimes in China and elsewhere in the world to cruelly exploit and abuse their own citizens.

Over the years, I have held 25 hearings on human rights abuses in China, and while China's economy has improved somewhat, the human rights situation remains abysmal. So-called economic reform has utterly failed to result in the protection of freedom of speech, expression, or assembly. The Laogai system of forced labor camps is still full with an estimated 6 million people; the Chinese government permits a horrifying trade in human organs; the PRC's draconian one-child per couple policy has made brothers and sisters illegal and coerced abortion commonplace; and political and religious dissidents are systematically persecuted and tortured.

Similarly, while the internet has opened up commercial opportunities and provided access to vast amounts of information for people the world over, the internet has also become a malicious tool: a cyber sledgehammer of repression of the government of China. As soon as the promise of the Internet began to be fulfilled – when brave Chinese began to email each other and others about human rights issues and corruption by government leaders - the Party cracked down. To date, an estimated 49 cyber-dissidents and 32 journalists have been imprisoned by the PRC for merely posting information on the Internet critical of the regime. And that's likely to be only the tip of the iceberg.

Tragically, history shows us that American companies and their subsidiaries have provided the technology to crush human rights in the past. Edwin Black's book *IBM and the Holocaust* reveals the dark story of IBM's strategic alliance with Nazi Germany. Thanks to IBM's enabling technologies, from programs for identification and cataloging to the use of IBM's punch card technology, Hitler and the Third Reich were able to automate the genocide of the Jews.

U.S. technology companies today are engaged in a similar sickening collaboration, decapitating the voice of the dissidents. In 2005, Yahoo's cooperation with Chinese secret police led to the imprisonment of the cyber-dissident Shi Tao. And this was not the first time. According to Reporters Without Borders, Yahoo also handed over data to Chinese authorities on another of its users, Li Zhi . Li Zhi was sentenced on December 10, 2003 to eight years in prison for "inciting subversion." His "crime" was to criticize in online discussion groups and articles the well-known corruption of local officials.

Women and men are going to the gulag and being tortured as a direct result of information handed over to Chinese officials. When Yahoo was asked to explain its

actions, Yahoo said that it must adhere to local laws in all countries where it operates. But my response to that is: if the secret police a half century ago asked where Anne Frank was hiding, would the correct answer be to hand over the information in order to comply with local laws? These are not victimless crimes. We must stand with the oppressed, not the oppressors.

I was recently on a news show talking about Google and China. The question was asked, "Should it be business' concern to promote democracy in foreign nations?" That's not necessarily the right question. The more appropriate question today is, "Should business enable the continuation of repressive dictatorships by partnering with a corrupt and cruel secret police and by cooperating with laws that violate basic human rights?"

I believe that two of the most essential pillars that prop up totalitarian regimes are the secret police and propaganda. Yet for the sake of market share and profits, leading U.S. companies like Google, Yahoo, Cisco and Microsoft have compromised both the integrity of their product and their duties as responsible corporate citizens. They have aided and abetted the Chinese regime to prop up both of these pillars, propagating the message of the dictatorship unabated and supporting the secret police in a myriad of ways, including surveillance and invasion of privacy, in order to effectuate the massive crackdown on its citizens.

Through an approach that monitors, filters, and blocks content with the use of technology and human monitors, the Chinese people have little access to uncensored information about any political or human rights topic, unless of course, Big Brother wants them to see it. Google.cn, China's search engine, is guaranteed to take you to the virtual land of deceit, disinformation and the big lie. As such, the Chinese government utilizes the technology of U.S. IT companies combined with human censors - led by an estimated force of 30,000 cyber police - to control information in China. Websites that provide the Chinese people news about their country and the world, such as BBC, much of CNN, as well as Voice of America and Radio Free Asia, are regularly blocked in China. In addition, when a user enters a forbidden word, such as "democracy," "China torture" or "Falun Gong," the search results are blocked, or you are redirected to a misleading site, and the user's computer can be frozen for unspecified periods of time.

Cisco has provided the Chinese government with the technology necessary to filter internet content through its creation of Policenet, one of the tools the regime uses to control the internet. Cisco holds 60 percent of the Chinese market for routers, switches, and other sophisticated networking gear, and its estimated revenue from China, according to Derek Bambauer of *Legal Affairs*, is estimated to be \$500 million annually. Yet Cisco has also done little creative thinking to try to minimize the likelihood that its products will be used repressively, such as limiting eavesdropping abilities to specific computer addresses.

Similarly, Google censors what are euphemistically called "politically sensitive" terms, such as "democracy," "China human rights," "China torture" and the like on its new Chinese search site, Google.cn. Let's take a look at what this means in practice. A

search for terms such as "Tiananmen Square" produces two very different results. The one from Google.cn shows a picture of a smiling couple, but the results from Google.com show scores of photos depicting the mayhem and brutality of the 1989 Tiananmen square massacre. Another example: let's look at "China and torture." Google has said that some information is better than nothing. But in this case, the limited information displayed amounts to disinformation. A half truth is not the truth – it is a lie. And a lie is worse than nothing. It is hard not to draw the conclusion that Google has seriously compromised its "Don't Be Evil" policy. It has become evil's accomplice.

Not surprisingly, Americans, not just Chinese, are also the victims of this censorship. On an informal request from the Chinese government, Microsoft on December 30, 2005 shut down the blog of Zhao Jing because the content of Zhao's blog on MSN Spaces was offensive to the PRC. Zhao had tried to organize a walk-off of journalists at the *Beijing News* after their editor was fired for reporting on clashes between Chinese citizens and police in southern China. However, Microsoft shut down the blog not only in China, but everywhere. It not only censored Chinese access to information, but American access to information, a step it has only recently pulled back from. Like Yahoo, MSN defended its decision by asserting that MSN is committed to complying with "*local* laws, norms, and industry practices in China." Regrettably, I haven't been able to find an MSN statement on its commitment to *global* laws, norms, and industry practices protecting human rights in China.

Standing for human rights has never been easy or without cost. It seems that companies have always resisted having to abide by ethical standards, yet we have seen the success of such agreements as the Sullivan principles in South Africa and MacBride principles in Northern Ireland. I, and many of my colleagues on both sides of the aisle, would welcome leadership by the corporations to develop a code of conduct which would spell out how they could operate in China and other repressive countries while not harming citizens and respecting human rights. But I believe our government also has a major role to play in this critical area, and that a more comprehensive framework is needed to protect and promote human rights. This is why I intend to introduce The Global Online Freedom Act of 2006 in the coming week to promote freedom of expression on the internet.

There are some encouraging and innovative public and private efforts already underway in this area. Electronic Frontier Foundation, for instance, allows Windows-based computers to become proxies for internet users, circumventing local Internet restrictions. Through the efforts of the U.S. Broadcasting Board of Governors' fund of a mere \$100,000, VOA and Radio Free Asia's websites are accessible to Chinese internet users through proxy servers because of the technology of Dynaweb and UltraReach.

Earlier this month, the technology firm Anonymizer announced that it is developing a new anti-censorship technology that will enable Chinese citizens to safely access the entire Internet filter-free. The solution will provide a regularly changing URL so that users can likely access the uncensored internet. In addition, users' identities are apparently protected from online monitoring by the Chinese regime. Lance Cottrell of

Anonymizer said it "is not willing to sit idly by while the freedom of the Internet is slowly crushed. We take pride in the fact that our online privacy and security solutions provide access to global information for those under the thumb of repressive regimes."

In conclusion, I hope this hearing might be the beginning of a different sort of dialogue – a discussion on how American high-tech firms can partner with the U.S. government and human rights activists to bring down the Great Firewall of China, and on how America's greatest software engineers can use their intelligence to create innovative new products to protect dissidents and promote human rights.

John Aird Statement

I would like to take this opportunity to recognize and honor the work of Dr. John S. Aird, a distinguished American whose immeasurable contributions as a scholar, population expert, and defender of human rights have changed the lives of so many over the course of his career.

It was with great sadness that I learned of Dr. Aird's death last October. His passing represents a grave loss for all of us who are committed to ensuring human rights around the world, and his tremendous work in this and other fields will not be forgotten.

Dr. Aird, former Senior Research Specialist on China at the U.S. Census Bureau, served for 28 years as that organization's resident expert on the population of China. He was a forthright and vehement critic of the Chinese government's coercive one-child family planning policy.

During his retirement, Dr. Aird worked as a full-time volunteer. He provided expert testimony in immigration courts for 415 families, helping Chinese citizens fleeing their country's coercive family planning programming to secure asylum in the United States.

John S. Aird was truly one of the most informed and outspoken opponents of China's one-child policy. He testified before this and other Congressional committees on numerous occasions, and I believe my colleagues would join me in saying that his insights were consistently persuasive and well-considered, and proved invaluable to our work on human rights in China.

I would also like to acknowledge today the presence of Dr. Aird's wife of more than 58 years, Mrs. Laurel J. Aird, who has graciously joined us for this important hearing which will continue the course on human rights in China that Dr. Aird helped to chart with his work.